

a<sup>1</sup>  
don't 6. (Amended-Clean Copy) A method as claimed in Claim 1 wherein the bit pattern is generated from the features using a representation scheme.

---

8. (Amended-Clean Copy) A method as claimed in Claim 1 wherein the image is a fingerprint image and the features measures are of minutiae points.

---

a<sup>2</sup> 9 (Amended-Clean Copy) A method as claimed in Claim 1 wherein the image is a face image and the feature measures are of corners of the image.

---

10. (Amended-Clean Copy) A method as claimed in Claim 1 wherein the associative memory is implemented using a neural network.

---

a<sup>3</sup> 12. (Amended-Clean Copy) A method as claimed in Claim 1 wherein, in step (5), a symmetry key or public/private key pair is generated.

---

a<sup>4</sup> 14. (Amended-Clean Copy) A method as claimed in Claim 1 wherein steps (1) - (4) are applied to a plurality of biometrics data sources, the key being generated from a respective plurality of retrieved bit patterns.

---

a<sup>5</sup> 16. (Amended-Clean Copy) A method as claimed in Claim 1 wherein a plurality of keys corresponding to a plurality of persons are generated and the corresponding bit patterns are stored in two or more parallel associative memories.

---

17. (Amended-Clean Copy) A method as claimed in Claim 1 wherein step (1) is performed a plurality of times to provide a plurality of samples and only invariant feature measures persistent in all samples are used to generate the key.

---